Isomorfimos sobre Anéis de Grupo Inteiro

Andréa Luiza Gonçalves Martinho

Janeiro de 2007

UFRJ

Isomorfimos sobre Anéis de Grupo Inteiro

por

Andréa Luiza Gonçalves Martinho

Dissertação de Mestrado apresentada ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientador: Guilherme Leal

Rio de Janeiro

Janeiro de 2007

Martinho, Andrea Luiza Gonçalves.

M385 Isomorfimos sobre Anéis de Grupo Inteiro/Andrea Luiza Gonçalves Martinho.-

Rio de Janeiro: UFRJ/IM, 2007.

v,50f.; 30 cm

Orientador: Guilherme Augusto de La Rocque Leal.

Dissertação(Mestrado) - UFRJ/IM. Programa de Pós-Graduação em Matemática, 2010.

Bibliográfia: p.41.

1. Anéis de grupo - tese. 2. Isomorfismo (Matemática) I. Leal, Guilherme Augusto de La Rocque. II. Universidade Federal do Rio de Janeiro. Instituto de Matemática.

Isomorfimos sobre Anéis de Grupo Inteiro

por

Andréa Luiza Gonçalves Martinho

Dissertação submetida ao Corpo Docente do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para a obtenção do grau de Mestre em Matemática.

Área de concentração: Matemática

Aprovada por:

Prof. Dr. Guilherme Leal - UFRJ
(Presidente)

Prof. Dr. Osnel Broche Cristo - UFLA

Prof. Dr. Adilson Gonçalves- UFRJ

Prof. Dr. Franscico César P. Milies - USP

Rio de Janeiro

Janeiro de 2007

Isomorfimos sobre Anéis de Grupo Inteiro

Andréa Luiza Gonçalves Martinho

Orientador: Guilherme Leal

Resumo

Resumo da Dissertação submetida ao Programa de Pós-graduação em Matemática, Instituto de Matemática, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

O objetivo desta dissertação é estudar os isomorfismos dos anéis de grupo inteiro; veremos que se G é um grupo nilpotente de classe dois, qualquer automorfismo dos anéis de grupo inteiro é composto de um automorfismo de G e um automorfismo interno por uma unidade adequada da álgebra de grupo de G com coeficientes racionais. Além disso, provaremos uma extensão do resultado clássico de Higman para o caso de grupos abelianos finitos. Finalmente, construiremos um isomorfismo de anéis de grupos inteiro de grupos finitos que preserva o reticulado de subgrupos normais.

Rio de Janeiro

Janeiro de 2007

Isomorfimos sobre Anéis de Grupo Inteiro

Andréa Luiza Gonçalves Martinho

Orientador: Guilherme Leal

Abstract

Abstract da Dissertação submetida ao Programa de Pós-graduação em Matemática, Instituto de Matemática, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

The objective of this dissertation is to study the isomorphisms of group rings over, we see that if G is a nilpotent group of class two, any automorphism of the ring the whole group is composed of an automorphism of G and an automorphism procedure by an appropriate unit of the group algebra of G with rational coefficients. Furthermore, prove an extension of the classical result of Higman for the case of finite abelian groups. Finally, we will construct an isomorphism of groups over rings of finite groups which preserves the lattice of normal subgroups.

Rio de Janeiro

Janeiro de 2007

Agradecimentos

Agradeço a Deus por ter me dado força e coragem
para superar mais essa etapa de minha vida.
Agradeço aos meus filhos Irapuan e Leandro
pelo carinho e amor, que sem o qual não poderia viver.
Agradeço ao meu marido Leandro Tomaz de Araujo
que sua constante determinação nunca me deixou esmorecer.
Agradeço aos meus pais Irapuan e Rita,
que sempre estiveram ao meu lado em todos os momentos.

Rio de Janeiro,
Andréa Luiza G. Martinho

.

Para meus filhos

Irapuan e Leandro.

Sumário

1 Preliminares **3**

1.1 Anéis de grupo 3

1.2 Ideais de Aumento 6

1.3 Semisimplicidade 9

2 Automorfismos dos anéis de grupo inteiro **21**

3 Isomorfismos dos anéis de grupos inteiro de grupos abelianos finitamente gerados **30**

4 Idempotentes centrais e subgrupos normais **33**

4.1 Fatos Importantes 33

4.2 Teorema de Preservação e Existência 38

Referências Bibliográficas **41**

Introdução

O surgimento do conceito de anéis de grupo foi de uma forma implícita no artigo de A. Cayley [7], que é considerado o primeiro trabalho na teoria abstrata de grupos. Em 1897, T. Molin explicitou esse conceito. No ano de 1947, na conferência de Álgebra de Michigan, R.M. Thrall formulou o seguinte problema:

> **Problema do Isomorfismo:** Dados um grupo G e um corpo K, determinar todos os grupos H, tais que $KG \cong KH$.

Na mesma época, S. Perlis e G. Walker reformulou este problema da seguinte maneira:

> Dados dois grupos finitos de mesma ordem n, determinar quais corpos K, tem-se $KG \cong KH$.

O trabalho desenvolvido pelos mesmos, mostrou que para grupos abelianos finitos os quais a característica do corpo não divide a ordem do grupo, a resposta é sempre positiva neste caso. Todavia, Mazur pensou no problema do Isomorfismo de forma mais geral; a saber, será que a existência de um isomorfismo entre as R-algebras RG e RH implicará na existência de um isomorfismo entre os grupos G e H? Para anéis de grupo inteiro de grupos abelianos finitos, está questão foi respondida aproximadamente em 1940, por G. Higman.

Hertwerck deu um contra-exemplo para esta conjectura para anéis de gupos finitos. Mas o desáfio de saber para quais classes de grupos esta conjectura é válida continuou sendo de interesse para os matemáticos. Desta forma, Roggenkamp

e Scott responderam esta questão para anéis de grupo inteiro de grupos nilpotentes finitos, e Wchitcomb para anéis de grupos inteiros de grupos metabelianos. Todavia, para grupos infinitos ainda pouco se sabe; e nem mesmo se a classe de nilpotência é preservada. Mas sabemos que para anéis de grupo inteiro de grupos abelianos finitamente gerados esta conjectura é válida, que é:

Sejam G e H grupos abelianos finitamente gerados então

$$\mathbb{Z}G \simeq \mathbb{Z}H \Rightarrow G \simeq H. \quad (1)$$

No capítulo 1, apresentaremos os resultados básicos de anéis de grupo, ideais de aumento e semisimplicidade, que serão utilizados nos capítulos posteriores. Finalizaremos o mesmo enunciando alguns teoremas, os quais omitiremos as demonstrações.

No capítulo 2, utilizando o **Teorema de Glauberman** provaremos que se G é um grupo nilpotente de classe dois, qualquer automorfismo de $\mathbb{Z}G$ é composto de um automorfismo interno por uma unidade adequada de $\mathbb{Q}G$, a álgebra de grupo de G com coeficientes racionais.

No capítulo 3, primeiro caracterizaremos as unidades de ordem finita de um grupo abeliano finitamente gerado e depois provaremos o resultado (1).

No último capítulo, construiremos um isomorfismo de anéis de grupos inteiro de grupos finitos que preserva o reticulado de subgrupos normais.

No presente trabalho, baseado no artigo [9], estudaremos o conceito de anéis de grupo, onde o anel em questão será o anel dos Inteiros, que recebe o nome de **Anel de Grupo Inteiro**.

Capítulo 1

Preliminares

1.1 Anéis de grupo

Seja G um grupo (não nessessariamente finito) e R um anel com unidade. O nosso objetivo é construir um R-módulo, tendo os elementos de G como base, e então usar as operações de G e de R para definir uma estrutura de anel. Assim, denotaremos por RG o conjunto de todas as combinações lineares da forma $\alpha = \sum_{g \in G} \alpha_g g$, onde $\alpha_g \in R$ e $\alpha_g = 0$ quase sempre, isto é, somente um número finito de coeficientes são diferentes de 0 em cada uma dessas somas.

Definição 1.1. *Dado um elemento $\alpha = \sum_{g \in G} \alpha_g g \in RG$, definimos o suporte de α como sendo o subconjunto dos elementos de G que aparecem efetivamente em α, que é:*

Observação 1.2. .

1. *Usaremos a seguinte notação: $supp(\alpha) = \{g \in G : \alpha_g \neq 0\}$.*

2. *Segue da definição que: dados dois elementos α e β de RG, isto é, $\alpha = \sum_{g \in G} \alpha_g g$ e $\beta = \sum_{g \in G} \beta_g g$, temos que $\alpha = \beta$ se e somente se $\alpha_g = \beta_g$, $\forall g \in G$.*

Definição 1.3. *Dado dois elementos* $\alpha = \sum_{g\in G} \alpha_g g$ *e* $\beta = \sum_{g\in G} \beta_g g$ *em* RG *definimos soma por:*

$$\alpha + \beta = \left(\sum_{g\in G} \alpha_g g\right) + \left(\sum_{g\in G} \beta_g g\right) = \sum_{g\in G} (\alpha_g + \beta_g) g.$$

Definição 1.4. *Dado dois elementos* $\alpha = \sum_{g\in G} \alpha_g g$ *e* $\beta = \sum_{g\in G} \beta_g g$ *em* RG *definimos produto por:*

$$\alpha\beta = \left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{g\in G} \beta_g g\right) = \sum_{g,h\in G} \alpha_g \beta_h gh.$$

Observação 1.5. .

1. *Se* $c_v = \sum_{gh=v} \alpha_g \beta_g$, *então reordenando os termos na expressão acima, temos o produto* $\alpha\beta$ *como:* $\alpha\beta = \sum_{v\in G} c_v v$.
2. *Com as operações definidas anteriormente, é podemos verificar que* RG *é um anel com unidade; a saber, o elemento* $\mathbf{1} = \sum_{g\in G} u_g g$, *onde o coeficiente correspondente ao elemento unidade do grupo é igual a* 1 *e* $u_g = 0$ *para todos* $g \in G$, $g \neq 1$.

Definição 1.6. *Dado um* $\alpha = \sum_{g\in G} \alpha_g g \in RG$ *podemos definir o produto de* α *por* $\lambda \in R$ *como*

$$\lambda\alpha = \lambda\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} (\lambda\alpha_g) g.$$

Novamente, é podemos verificar que RG é um R-módulo. E temos que se R é comutativo com unidade, segue que RG é uma álgebra sobre R.

Definição 1.7. *O conjunto* RG, *com as operações definidas anteriormente, é chamado anel de grupo de* G *sobre* R. *No caso em que* R *é comutativo* RG *é chamado a álgebra de grupo de* G *sobre* R.

Agora, definimos a seguinte aplicação

$$\begin{array}{rcl} \varepsilon : RG & \longrightarrow & R \\ \sum_{g\in G} a_g g & \longmapsto & \sum_{g\in G} a_g. \end{array}$$

Observe que a aplicação definida acima é um homomorfismo de anéis. O que motiva a seguinte definição:

Definição 1.8. .

1. *O homomorfismo* ε*, com definido acima é chamado de aplicação de aumento de* RG*.*

2. *O núcleo de* ε *é chamado de ideal de aumento de* RG*, que denotamos por* $\Delta(G)$*.*

A definição acima desempenha um papel central nessa dissertação. E estes ideais de aumento serão caracterizados na seção 2.2.

Observação 1.9. .

1. *Dados* $\alpha = \sum_{g\in G} \alpha_g g \in \Delta(G)$*, temos* $\varepsilon(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} \alpha_g = 0$*. Assim, podemos escrever* α *na forma:*

$$\alpha = \sum_{g\in G} \alpha_g g - \sum_{g\in G} \alpha_g = \sum_{g\in G} \alpha_g (g-1).$$

2. *Os elementos da forma* $g-1 \in \Delta(G)$*, onde* $g \in G$*. Assim,* $\mathcal{G} = \{g-1 \ : \ g \in G, g \neq 1\}$ *é um conjunto de geradores de* $\Delta(G)$ *sobre* R*.*

3. *O conunto* $\mathcal{G}$ *é linearmente independente, pois os elementos de* $\mathcal{G}$ *são linearmente indendentes.*

Proposição 1.10. *O conjunto* $\mathcal{G}$ *é uma base de* $\Delta(G)$ *sobre* R*.*

Demonstração. Segue da observação anterior. □

Assuma que somente uma quantidade finita de elementos α_g são diferentes de zero, então pela proposição anterior, temos:

$$\Delta(G) = \left\{ \sum_{g\in G} \alpha_g (g-1) \ : \ g \in G \ , \ g \neq 1 \ , \ \alpha_g \in R \right\}$$

Em particular, se R é anel comutativo e G é um grupo finito, então $\Delta(G)$ é um R-módulo livre de posto $|G|-1$.

Proposição 1.11. *Seja R um anel comutativo. A aplicação* $^* : RG \longrightarrow RG$ *definida por*

$$\left(\sum_{g\in G} \alpha_g g\right)^* = \sum_{g\in G} \alpha_g g^{-1}$$

satisfaz as seguintes propriedades:

(i) $(\alpha+\beta)^* = \alpha^* + \beta^*$,

(ii) $(\alpha\beta)^* = \beta^*\alpha^*$,

(iii) $\alpha^{**} = \alpha$, *e*

(iv) $(\lambda\alpha)^* = \lambda\alpha^*$.

Demonstração. É imediata □

O resultado anterior, mostra que dado um anel de grupo sobre um anel comutativo RG, sempre podemos considerar RG um anel de evolução.

1.2 Ideais de Aumento

Dado um grupo G e um anel R , vamos denotar por $\mathcal{S}(G)$ o conjunto de todos os subgrupos de G.

Definição 1.12. *Para um subgrupo $H \in \mathcal{S}(G)$, denotaremos por $\Delta_R(G,H)$ o ideal de RG gerado pelo conjunto $\{h-1 \,:\, h \in H\}$. Isto é,*

$$\Delta_R(G,H) = \{\sum_{h\in H} \alpha_h(h-1) : \alpha_h \in RG\}.$$

Por simpicidade, omitiremos o índice R quando não houver dúvidas quanto ao anel R, e denotaremos o ideal simplismente por $\Delta(G,H)$.

Observação 1.13. *Tomando $H = G$ na definição anterior vemos claramente que $\Delta(G,G)$ coincide com o ideal $\Delta(G)$ introduzido na seção anterior.*

Lema 1.14. *Seja H um subgrupo de G e seja S um conjunto de geradores de H. Então, o conjunto $\{\ s-1\ :\ s \in S\}$ é um conjunto de geradores de $\Delta(G,H)$ como um ideal à esquerda de RG.*

Demonstração. Ver [8, Pag, 135]. □

Nosso objetivo é dar uma melhor descrição de $\Delta(G,H)$, então vamos denotar por $\mathcal{T} = \{q_i\}_{i\in I}$ um conjunto completo dos representantes das classes à esquerda de H em G, que é chamado **transversal** de H em G. Como um representante de H em $\mathcal{T}$ estamos escolhendo precisamente o elemento identidade de G. Portanto todo elemento $g \in G$ pode ser escrito de forma única como $g = q_i h_j$ com $q_i \in \mathcal{T}$ e $h_j \in H$.

Proposição 1.15. *O conjunto $B_H = \{q(h-1) : q \in \mathcal{T}, h \in H, h \neq 1\}$ é uma base de $\Delta_R(G,H)$ sobre R.*

Demonstração. Primeiro, mostraremos que B_H é linearmente independente sobre R. Assuma que temos uma combinação linear nula, isto é,

$$\sum_{i,j} r_{ij} q_i (h_j - 1) = 0, r_{ij} \in R.$$

Então, podemos escrever:

$$\sum_{i,j} r_{ij} q_i h_j = \sum_i \left(\sum_j r_{ij} \right) q_i.$$

Como $h_j \neq 1$ para todos os valores de j, segue que os membros na equação acima tem suportes disjuntos. E como os elementos de G são linearmente independentes sobre R, segue facilmente que todos os coeficientes devem ser 0. Em particular, $r_{ij} = 0$, para todo i, j. Agora, para mostrar que B_H gera $\Delta_R(G,H)$ é suficiente provar que todo elemento da forma $g(h-1)$, com $g \in G$, $h \in H$, pode ser escrito como uma combinação linear dos elementos de B_H. Agora, $g = q_i h_j$ para algum $q_i \in \mathcal{T}$ e algum $h_j \in H$. Então

$$g(h-1) = q_i h_j (h-1) = q_i (h_j h - 1) - q_i (h_j - 1).$$

□

Agora, daremos uma outra interpretação para $\Delta(G, H)$ onde H é um subgrupo normal de G. Se $H \triangleleft G$, então o homomorfismo canônico $w : G \to G/H$ pode ser extendido para um epimorfismo $w^* : RG \to R(G/H)$ tal que

$$w^* \left(\sum_{g \in G} \alpha_g g \right) = \sum_{g \in G} \alpha_g w(g).$$

Denotaremos por $Ker(w^*)$ o núcleo de w^*.

Proposição 1.16. *Com a notação acima, Ker* $(w^*)= \Delta(G, H)$.

Demonstração. Seja $\mathcal{T}$ uma transversal de H em G. Então, todo elemento $\alpha \in RG$ pode ser escrito como uma soma finita:

$$\alpha = \sum_{i,j} r_{ij} q_i h_j, \ \textit{com } r_{ij} \in R, \ q_i \in \mathcal{T} \textit{ e } h_j \in H.$$

Se denotarmos por $\overline{q_i}$ a imagem de q_i no grupo quociente G/H, então temos que

$$w^*(\alpha) = \sum_i \left(\sum_j r_{ij} \right) \overline{q_i}$$

Logo, $\alpha \in Ker(w^*)$ se e somente se $\sum_{i,j} r_{ij} = 0$ para cada valor de i. Assim, se $\alpha \in Ker(w^*)$ podemos escrever:

$$\alpha = \sum_{i,j} r_{ij} q_i h_j = \sum_{i,j} r_{ij} q_i h_j - \sum_i \left(\sum_j r_{ij} \right) q_i =$$

$$= \sum_{i,j} r_{ij} q_i (h_j - 1) \in \Delta(G, H)$$

Portanto, $Ker(w^*) \subset \Delta(G, H)$. A inclusão contrária segue trivialmente.

□

Corolário 1.17. *Seja H um subgrupo normal de G. Então, $\Delta(G, H)$ é um ideal de RG e*

$$\frac{RG}{\Delta(G, H)} \simeq R(G/H).$$

Observação 1.18. *Podemos ver que $\Delta(G)$ é o núcleo do epimorfismo ε induzido pele aplicação trivial $G \to G/G = \{1\}$.*

1.3 Semisimplicidade

Nesta seção queremos determinar condições necessárias e suficientes sobre R e G para que o anel RG seja semisimples Artiniano. Para tal, precisaremos de algumas definições e resultados preliminares como os que segue.

Definição 1.19. *Sejam N e N' submódulos de um R-módulo M. Denotaremos por $\mathbf{S}(M)$ a coleção de submódulos de M. Então N é chamado de completamento de N' em $\mathbf{S}(M)$ se M é igual a soma direta de N e N', isto é, $M = N \oplus N'$, ou seja $M = N + N'$ e $N \cap N' = (0)$. Neste caso podemos também dizer que M é uma soma direta de N e N', ou N é um somando direto de M.*

Definição 1.20. .

1. *Um R-módulo M é chamado complementado se todo submódulo $N \neq 0$ de M tem um completamento.*
2. *Um R-módulo M é chamado completamente redutível se M é a soma de submódulos simples à esquerda de M.*

Sabemos que todo submódulo $N \neq 0$ de M tem um completamento se e somente se M é a soma de submódulos simples à esquerda de M. Para ver a prova desse fato veja [8]. Podemos dizer então que M é um R-módulo completamente redutível se todo submódulo de M é tem um completamento. Em consequência disso, temos que M é um R-módulo completamente redutível se e somente se M é a soma direta de submódulos simples de M.

Observação 1.21. *Os submódulos de um anel R visto como R-módulo à esquerda são os ideais à esquerda do anel R, segue então que R é complemente redutível se e somente se R é a soma de ideais minimais à esquerda, ou seja se todo ideal à esquerda tem um complemento. Em consequência disso, temos que R é completamente redutível se e somente se R é a soma direta de ideais minimais à esquerda do anel R.*

Vamos agora provar um teorema que será de fundamental importância na demonstração do teorema 1.31, além de caracterizar anéis (vistos como R-módulos) completamente redutíveis.

Teorema 1.22. *Seja R um anel. Então R é completamente redutível se e somente se R é a soma de um número finito de ideais minimais á esquerda de R.*

Demonstração. Se R é a soma de um número finito de ideais minimais á esquerda de R, pela definição 1.20 temos que R é completamente redutível. Assuma que R é completamente redutível, isto é, $R = \sum_{i \in I} N_i$, onde $N_i' s$ são ideais minimais à esquerda de R. Assim para provar nossa equivalência basta mostrar que esta soma é finita. Em particular, o elemento $1 \in R$ e pode ser escrito como uma soma finita : $1 = x_{i_1} + ... + x_{n_i}$, com $x_{i_j} \in L_{i_j}$. Então para um elemento arbitrário $r \in R$, temos que $r = r.1 = rx_{i_1} + ... + rx_{n_i}$, onde $rx_{i_j} \in L_{i_j}$, $1 \leq j \leq n$. Isso mostra que $R \subset L_{i_1} + ... + L_{i_n}$. Como a inclusão contrária é óbvia, concluimos que $R = L_{i_1} + ... + L_{i_n}$. □

Definição 1.23. *Seja M um R-módulo. Dizemos que M satifaz a condição de cadeia descendente, denotada por (C.C.D.), se toda cadeia de submódulos de M:*

$$M_1 \supset M_2 \supset ... \supset M_i \supset ...$$

termina; isto é, se existe um índice i talque $M_i = M_{i+t}$ para todo inteiro positivo t. Se M satisfaz a (C.C.D.), dizemos que M é um módulo Artiniano. Um anel R é chamado Artiniano à esquerda se R visto como R-módulo à esqueda é Artiniano e Artiniano à direita se R visto como R-módulo à direita é Artiniano.

Definição 1.24. *Seja M um R-módulo. Dizemos que M satifaz a condição de cadeia descendente, denotada por (C.C.A.), se toda cadeia de submódulos de M:*

$$M_1 \subset M_2 \subset ... \subset M_i \subset ...$$

termina; isto é, se existe um índice i talque $M_i = M_{i+t}$ para todo inteiro positivo t. Se M satisfaz a (C.C.A.), então dizemos que M é um módulo Noetheriano.

Um anel R é chamado Noetheriano à esquerda se R visto como R-módulo à esqueda é Noetheriano e Noetheriano à direita se R visto como R-módulo à direita é Noetheriano.

Definição 1.25. *Uma cadeia de submódulos de um R-módulo M:*

$$M = M_0 \supset M_1 \supset ... \supset M_n = (0)$$

é chamada série de composição de M se todo módulo M_i/M_{i+1} são simples. Esses são chamados de fatores da série. O número de fatores é chamado de tamanho da série. Um módulo tendo uma série de composição é dito ser de tamanho finito.

Provaremos um teorema que fornece condições necessárias e suficientes para a existência de uma série de composição. Todavia, primeiro provaremos o seguinte lema.

Lema 1.26. *Seja N um submódulo de um R-módulo M. Então, M é Noetheriano (Artiniano) se e somente se N e M/N são Noetheriano (Artiniano).*

Demonstração. Assuma primeiro que N e M/N são Noetheriano e seja

$$M_1 \subset M_2 \subset ... \subset M_i \subset ... \tag{1.1}$$

uma cadeia ascendente de submódulos de M. Consideremos as seguintes cadeias:

$$(M_1 \cap N) \subset (M_2 \cap N) \subset ... \subset (M_i \cap N) \subset ...$$

$$\frac{(M_1 + N)}{N} \subset \frac{(M_2 + N)}{N} \subset ... \subset \frac{(M_i + N)}{N} \subset ...$$

Como N e M/N são Noetherianos, as duas cadeias acima terminam. Podemos assim determinar um inteito positivo k tal que para todo $i \geq k$ temos

$$M_i \cap N = M_k \cap N$$

$$M_i + N = M_k + N$$

É facil ver que $M_k \subset M_i$ se $i \geq k$; queremos mostrar que a inclusão contrária também é verdadeira. Dado um elemento $x \in M_i$, a segunda igualdade acima mostra que existe $y \in M_k$ tal que $x + N = y + N$, então $x - y \in N$. Como $M_k \subset M_i$, temos que $x - y \in M_i \cap N = M_k \cap N$. Portanto, $x - y \in M_k$ e $x \in M_k$. Logo $M_k = M_i$ para todo $i \geq k$ e a cadeia 1.1 termina. A prova para o caso Artiniano é análoga, e a implicação contrária é imediata. □

Teorema 1.27. *Um R-módulo M é de tamanho finito se e somente se é Artiniano e Noetheriano.*

Demonstração. Assuma primeiro que M é Artiniano e Noetheriano. Sendo Noetheriano, a família de todos os submódulos próprios de M contém um elemento maximal M_1. Analogamente, $M_1 \neq (0)$ então M_1 contém um submódulo maximal M_2. Repetindo esse processo, podemos determinar uma cadeia de submódulos:

$$M = M_0 \supset M_1 \supset M_2 \supset ...$$

Como M é também Artiniano, a cadeia obrigatóriamente termina, então $M_n = (0)$ para algum inteiro positivo n. Então

$$M = M_0 \supset M_1 \supset M_2 \supset ... \supset M_n = (0)$$

é uma série de composição. Reciprocamente, assuma que M tem uma série de composição. Usaremos indução no tamanho n de uma série de composição de tamanho mininal de M. Se $n = 1$ então M é simples e assim Artiniano e Noetheriano. Assuma que

$$M = M_0 \supset M_1 \supset M_2 \supset ... \supset M_n = (0)$$

é um série de composição de tamanho minimal de M e que o resultado é válido para qualquer módulo contendo uma série de tamnho $n - 1$.

Como $M_1 \supset M_2 \supset ... \supset M_n = (0)$ é um série de composição de M_1, segue, pela hipótese de indução, que M_1 é Artiniano e Noetheriano. Como M/M_1 é

simples, M/M_1 é também Artiniano e Noetheriano então, pelo lema anterior, M é Artiniano e Noetheriano. □

Definição 1.28. *Seja R um anel.*

1. *O Radical de Jacobson de R, denotado por $J(R)$, é a interseção de todos os ideais maximais à esquerda de R.*
2. *Dizemos que R é semisimples se $J(R) = 0$.*

Agora, vamos caracterizar anéis semisimples Artinianos. Antes, provaremos uma proposição cujo corolário será uma ferramenta necessária na demonstração do teorema que vai mostrar essa caracterização.

Proposição 1.29. *Se I é um ideal minimal à esquerda de um anel R, então $I^2 = 0$ ou $I = Re$, onde e é um idempotente*[1] *de I.*

Demonstração. Assuma que $I^2 \neq 0$, então $Ib \neq 0$, para algum $b \in I$, logo $Ib = I$. Considere $B = \{r \in R \mid rb = 0\}$, então $B \cap I \neq I$, portanto $B \cap I = 0$. Agora, $eb = b$, para algum $e \in I$. Assim $(e^2 - e)b = 0$, e então $e^2 - e \in B \cap I = 0$. Portanto $e^2 = e$, e $e \neq 0$, pois $b \neq 0$. Então, $0 \neq Re \subset I$, e portanto $Re = I$. □

Corolário 1.30. *Todo ideal minimal à esquerda de um anel semisimples R é da forma Re, onde e é um idempotente de R.*

Teorema 1.31. *Seja R um anel, então R é semisimples Artiniano se somente se R é completamente redutível como R-módulo.*

Demonstração. Primeiro provaremos que se R é semisimples Artiniano então R é completamente redutível como R-módulo. Seja R é semisimples, isto é, a interseção de todos os ideais maximais à esquerda de R é 0. Como R é também Artiniano temos que esta interseção tem um número finito de ideais, isto é,

$$M_1 \cap M_2 \cap ... \cap M_n = 0.$$

[1]Um elemento e de um anel R é chamado idempotente se $e^2 = e$.

Podemos assumir que M_i não contém $A_i = \bigcap_{i \neq j} M_j$. Portanto,

$$R = M_i + A_i.$$

Em outras palavras, $M_i \cap A_i = 0$, portanto $A_i \cong R/M_i$, e para cada i, A_i é um R-módulo à esquerda simples, isto é, A_i é um ideal minimal de R. Assim, pelo corolário 1.30, temos $A_i = Re_i$, com $e_i^2 = e_i \in R$, e $M_i = R(e_i - 1)$. Seja $e = \sum_{i=1}^{n} e_i$, então

$$(e-1) = (e_i - 1) + \sum_{i \neq j} e_j \in M_i,$$

pois para $i \neq j$, temos que $e_j \in A_j \subset M_i$. Portanto, $e - 1 \in \bigcap_{i=1}^{n} M_i = 0$. Portanto, $1 = \sum_{i=1}^{n} e_i$, e assim $R = \sum_{i=1}^{n} A_i$ é completamente redutível.

Agora assuma que R é completamente redutível como R-módulo, então pelo teorema 1.22, temos que R é a soma de um número finito de ideais minimais à esquerda $I_1, I_2, ..., I_n$. Assim, temos uma série de composição

$$R = I_1 + I_2 + I_3 + ... + I_n \supset I_1 + I_2 + I_3 + ... + I_{n-1} \supset ... \supset I_1 + I_2 \supset I_1 \supset I_0 = (0)$$

de R, com R visto como R-módulo á esquerda, isto é, esta série de composição tem tamanho finito, então R é Artiniano. Agora, provaremos que R é semisimples. Seja R completamente redutível como R-módulo. Pela observação 1.21 podemos escrever R como soma direta de um número finito de ideais minimais à esquerda $I_1, I_2, ..., I_n$, isto é, $R = \oplus_{i=1}^{n} I_i$. Denote $N_j = \sum_{i \neq j} I_i$, onde $I_{i's}$ são ideais minimais à esquerda de R onde $1 \leq i \leq n$ e $1 \leq j \leq n$. Então $R/N_j \cong I_i$ e assim R/N_j é um ideal minimal à esquerda de R o que implica N_j é um ideal maximal à esquerda de R. Logo,

$$J(R) \subseteq \bigcap_j N_j = 0.$$

Portanto, $J(R) = 0$ e R é semisimples. $\square$

Visto que uma conição necessária e suficiente para que um R é semisimples Artiniano é que R é completamente redutível como R-módulo. Assim, teremos

uma caracterização de anéis semisimples Artinianos e iremos concluir a discussão sobre esse assunto. As definições que serão dadas a seguir são importantes para as identidades do lema 1.34 e em sua demonstração.

Definição 1.32. *Seja X um subconjunto de um anel de grupo RG.O anulador à esquerda de X é o conjunto*

$$Ann_l(X) = \{\alpha \in RG : \alpha x = 0, \forall x \in X\}$$

Analogamente, definimos o anulador à direita de X por:

$$Ann_r(X) = \{\alpha \in RG : x\alpha = 0, \forall x \in X\}$$

Agora, fixaremos uma importante notação será útil ao longo de toda dissertação.

Definição 1.33. *Dado um anel de grupo RG e um suconjunto finito Y do grupo G, denoteremos por $\widehat{Y}$ o seguinte elemento de RG:*

$$\widehat{Y} = \sum_{y \in Y} y.$$

Lema 1.34. *Seja H um subgrupo de G e R um anel. Então $Ann_r(\Delta(G, H)) \neq 0$ se e somente se H é finito. Neste caso, temos*

$$Ann_r(\Delta(G, H)) = \widehat{H}.RG.$$

Além disso, se $H \lhd G$, então o elemento $\widehat{H}$ é central em RG e temos

$$Ann_r(\Delta(G, H)) = Ann_l(\Delta(G, H) = RG.\widehat{H}.$$

Demonstração. Assuma que $Ann_r(\Delta(G, H)) \neq 0$ e escolha

$$\alpha = \sum_{g \in G} \alpha_g g \neq 0 \text{ em } Ann_r(\Delta(G, H)).$$

Para cada elemento $h \in H$ temos que $(h - 1)\alpha = 0$, então $h\alpha = \alpha$. Que é,

$$\alpha = \sum_{g \in G} \alpha_g g = \sum_{g \in G} \alpha_g hg$$

Tome $g_0 \in supp(\alpha)$. Então, $\alpha_{g_0} \neq 0$ assim a equação acima mostra que $hg_0 \in supp(\alpha)$ para todo $h \in H$. Como $supp(\alpha)$ é finito, isso implica que H é finito. Observe que se $g_0 \in supp(\alpha)$, então o coeficiente de todo elemento da forma hg_0 é igual ao coeficiente de g_0, assim podemos escrever α na forma:

$$\alpha = \alpha_{g_0}\widehat{H}g_0 + \alpha_{g_1}\widehat{H}g_1 + ...\alpha_{g_t}\widehat{H}g_t = \widehat{H}\beta,\ \beta \in RG.$$

O que mostra que , se H é finito, então $Ann_r(\Delta(G, H)) \subset \widehat{H}.RG$. A inclusão inversa segue trivialmente, pois $h\widehat{H} = \widehat{H}$ implica que $(h-1)\widehat{H} = 0$ para todo $h \in H$.

Finalmente, se $H \triangleleft G$ para qualquer $g \in G$ temos que $g^{-1}Hg = H$; portanto $g^{-1}\widehat{H}g = \sum_{h\in H} g^{-1}hg = \sum_{h \in H} h = \widehat{H}$ Assim, $\widehat{H}g = g\widehat{H}$, para todo $g \in G$, o que mostra que $\widehat{H}$ é central em G. Consequentemente, $RG.\widehat{H} = \widehat{H}.RG$ e o resultado segue. □

Corolário 1.35. *Seja G um grupo finito. Então*

1. *(i) $Ann_l(\Delta(G)) = Ann_r(\Delta(G)) = R.\widehat{G}$.*
2. *(ii)$Ann_r(\Delta(G)) \cap \Delta(G) = \{a\widehat{G}\ :\ a \in R,\ a|G| = 0\}$.*

Demonstração. (i) segue trivialmente do lema anterior tomando $H = G$. Para provar (ii) é suficiente notar que $\alpha = a\widehat{G} \in \Delta(G)$ se e somente se $\varepsilon(\alpha) = a\varepsilon(\widehat{G}) = a|G| = 0$. □

Lema 1.36. *Seja I um ideal de um anel R. Suponha que exista um ideal à esquerda J de R tal que $R = I \oplus J$ (como R-módulos à esquerda). Então, $J \subset Ann_r(I)$.*

Demonstração. Tome arbitrariamente elementos $x \in I$, $y \in J$. Como J é um ideal à esquerda e I é um ideal, temos que $xy \in J \cap I = (0)$. Consequentemente, $xy = 0$ e temos que $y \in Ann_r(I)$. □

Lema 1.37. *Se o ideal de aumento $\Delta(G)$ é um somando direto de RG como um RG- módulo então G é finito e $|G|$ é invertível, em R.*

Demonstração. Assuma que $\Delta(G)$ é um somando direto de RG. Então, o lema anterior mostra que $Ann_r(\Delta(G)) \neq 0$. Assim, pelo lema 1.34 e pelo corolário 1.35, G é finito e

$$Ann_r(\Delta(G)) = \hat{G}(RG) = \hat{G}R.$$

Escreva $RG = \Delta(G) \oplus J$ e $1 = e_1 + e_2$ com $e_1 \in \Delta(G)$ e $e_2 \in J$. Então $1 = \varepsilon(1) = \varepsilon(e_1) + \varepsilon(e_2)$. Como $J \subset Ann_r(\Delta(G))$ pelo lema anterior, temos então $e_2 = a\hat{G}$, para algum $a \in g$. Assim, $a\varepsilon(\widehat{G}) = 1$ e $a|G| = 1$. Isto mostra que $|G|$ é invertível em R e que $|G|^{-1} = a$. □

Agora, estamos prontos para determinar condições necessárias e suficientes em R e G para que o anel de grupo RG seja semisimples Artiniano.

Teorema 1.38 (Teorema de Maschke)**.** *Seja G um grupo e R um anel. Então, RG é semisimples Artiniano se e somente se as seguintes condições são verdadeiras:*

(i) R é um anel semisimples Artiniano.

(ii) G é finito.

(iii) $|G|$ é invertível em R.

Demonstração. Suponha que RG é semisimples Artiniano. Pelo corolário 2.15 e pela observação 2.16, temos que $\frac{RG}{\Delta(G)} \simeq R$. Como anéis de divisão de anéis semisimples Artinianos são sempre semisimples Artinianos, segue imediatamente que R é semisimples Artiniano. Para provar (i) e (ii) observemos que pelo teorema 2.32 RG é semisimples Artiniano, o que implica que RG é completamente redutível, pelo teorema 2.22, temos então que $\Delta(G)$ é um somado direto. Então pelo lema anterior, G é finito e $|G|$ é invertível em R. Reciprocamente, assuma que as condições (i), (ii) e (iii) são verdadeiras. Mostraremos que todo RG-submódulo é completamente redutível. Seja M um RG-submódulo de RG. Como R é semisimples Artiniano, segue que RG é semisimples Artiniano como

R-módulo e pelo teorema 2.32 temos que RG é completamente redutível. Assim, existe um R-módulo N de RG tal que

$$RG = M \oplus N.$$

O nosso objetivo é determinar um decomposição para RG, onde M aparece como RG-submódulo. Seja $\pi : RG \to M$ a projeção canônica associada à soma direta. Definimos $\pi^* : RG \to M$ como a média

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx), \ \forall x \in RG.$$

Se provarmos que π^* é, na realidade, um RG-homomorfismo talque $(\pi^*)^2 = \pi^*$ e $Im(\pi^*) = M$, então $Ker(\pi^*)$ será um RG-submódulo tal que $RG = M \oplus Ker(\pi^*)$ e assim o teorema estara provado. Como π^* é um R-homomorfismo, para mostrar que π^* é também um RG-homomorfismo é suficiente mostrar que

$$\pi^*(ax) = a\pi^*(x), \ \forall x \in G \ e \ \forall a \in G.$$

Então, temos que

$$\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi((ga)x).$$

Quando g percorre todos os elementos em G, o produto ga também percorre todos os elementos de G, assim

$$\pi^*(ax) = a\frac{1}{|G|} \sum_{g \in G} t^{-1}\pi(tx) = a\pi^*(x).$$

Como π é uma projeção em M, sabemos que $\pi(m) = m$, para todo $m \in M$. Além disso, como M é um RG-módulo, temos que $gm \in M$, para todo $g \in G$. Assim

$$\pi^*(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gm) = \frac{1}{|G|} \sum_{g \in G} g^{-1}gm = \frac{1}{|G|} \sum_{g \in G} m = \frac{|G|}{|G|}\, m \ = \ m.$$

Portanto, $M \subset Im(\pi^*)$. Agora, dado um elemento arbitrário $x \in RG$, temos que $\pi(gx) \in M$ para todo $g \in G$, pois $Im(\pi) = M$. Então

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx) \ \in M,$$

pois M é um RG-submódulo e então temos que $g^{-1}\pi(gx) \in M$. E segue que $Im(\pi^*) \subset M$. Portanto, $M = Im(\pi^*)$. Finalmente, como já vimos $\pi^*(x) \in M$, então

$$\pi^{*2}(x) = \pi^*(\pi^*(x)) = \pi^*(x), \ para\ todo\ x \in RG.$$

Logo, π^* é uma projeção. □

O caso onde $R = K$ é um corpo, temos que K é semisimples e $|G|$ é invertivel em K se, e somente se, $|G| \neq 0$ em K. Por outro lado, $|G| \neq 0$ se, e somente se, a característica de K não divide a ordem de G.

Corolário 1.39. *Seja G um grupo finito e seja K um corpo. Então, KG é semisimples Artiniano se e somente se caracteristica de K não divide $|G|$.*

Finalizaremos esta seção apresentando um descrição do centro de uma álgebra de grupo e enunciando alguns teoremas, ambas informações vamos utilizar nos capítulos subsequentes.

Definição 1.40. *Seja G um grupo, seja R um anel comutativo e seja $\{C_i\}_{i\in I}$ o conjunto de classes de conjugação de G que contém somente um número finito de elementos. Para cada índice $i \in I$ seja $\gamma_i = \widehat{C_i} = \sum_{x\in C_i} x$. Esse elementos são chamados de **somas de classe** de G sobre R.*

Teorema 1.41. *Seja G um grupo finito e R um anel comutativo. Então, o conjunto $\{\gamma_i\}_{i\in I}$ de todas as somas de classe forma uma base de $\mathcal{Z}(RG)$, o centro de RG, sobre R.*

Demonstração. Veja [8]. □

Teorema 1.42 (Teorema de Wedderburn)**.** *Seja A uma R-álgebra semisimples Artiniana.*

1. *Existe números naturais $n_1, ..., n_r$ e R-álgebras de divisão $D_1, ..., D_r$ tal que*

$$A \cong M_{n_1}(D_1) \oplus ... \oplus M_{n_r}(D_r).$$

2. *Os pares* $(n_1, D_1), ..., (n_r, D_r)$ *o qual 1 são determinados de maneira única (a menos de isomorfismo) por* A.

3. *Reciprocamente, se* $n_1, ..., n_r \in \mathbb{N}$ *e* $D_1, ..., D_r$ *são algebras de divisão sobre* R*, então* $M_{n_1}(D_1) \oplus ... \oplus M_{n_r}(Dr)$ *é uma* R*-álgebra semisimples Artiniana.*

Demonstração. Veja [8]. □

Teorema 1.43. *Seja* $R = \oplus_{i=1}^{s} A_i$ *uma decomposição de um anel semisimples Artiniano como soma direta de ideais minimais. Então, existe em família* $\{e_1, ..., e_s\}$ *de elementos de* R *tal que:*

1. $e_i \neq 0$ *é um indempotente central,* $1 \leq i \leq s$.

2. *Se* $i \neq j$ *então* $e_i e_j = 0$.

3. $1 = e_1 + ... + e_s$.

4. e_i *não pode ser escrito como* $e_i = e_i' + e_i''$ *onde* e_i', e_i' *são indepotentes centrais tais que* e_i', $e_i'' \neq 0$ *e* $e_i' e_i'' = 0$, $1 \leq i \leq s$.

Demonstração. Veja [8]. □

Definição 1.44. *Os elementos* $\{e_1, ..., e_s\}$ *no teorema acima são chamados idempotentes centrais primitivos de* R.

Teorema 1.45. *Seja* R *um anel. Então* R *é semisimples Artiniano se e somente se todo ideal á direita de* R *é da forma* $L = eR$*, onde* $e \in R$ *é um indepotente.*

Teorema 1.46. *(Teorema de Glauberman) Seja* $\theta : \mathbb{Z}G \to \mathbb{Z}H$ *um isomorfismo. Sejam* K_x *as somas de classe em* G*, isto é, soma dos conjugados distintos de um elemento* x *de* G*. Então* $\theta(K_x) = K_y$*, onde* K_y *é a soma de classes de conjungação em* H

Capítulo 2

Automorfismos dos anéis de grupo inteiro

Neste capítulo, nosso objetivo é provar que:

> *Se G é um grupo nilpotente de classe dois, então qualquer automorfismo de $\mathbb{Z}G$ é composto de um automorfismo interno por uma unidade de $\mathbb{Q}G$, a álgebra de grupo de G com coeficientes racionais.*

Para isso utilizaremos o *Teorema de Glauberman*, citado no capítulo anterior e duas proposições as quais serão provadas na sequência. Ainda, assumiremos que todos os grupos considerados neste capítulo são grupos finitos

Proposição 2.1. *Seja θ um automorfismo de $\mathbb{Z}G$. Sejam $C_{i's}$,$1 \leq i \leq r$ as classes de conjugação e $K_{i's}$ as correspondentes somas de classe de G. Suponha que $\theta(K_i) = K_{i'}$,$1 \leq i$,$i\prime \leq r$ e que exista um automorfismo σ de G tal que $\sigma(C_i) = C_{i'}$ para todo $1 \leq i \leq r$. Então existe uma unidade $\gamma \in \mathbb{Q}G$ tal que*

$$\theta(g) = \gamma g^{\sigma} \gamma^{-1}, \ \ \textit{para todo} \ \ g \in G.$$

Demonstração. Estendamos σ e θ de forma natural para $\mathbb{Q}$G. O centro de $\mathbb{Q}$G o qual é gerado pelas somas de classe K_i; $1 \leq i \leq r$; é fixo por $\sigma^{-1}\theta$. De fato, tomemos $\alpha \in \mathcal{Z}(\mathbb{Q}G)$ e definamos

$$\theta : \mathbb{Q}(G) \to \mathbb{Q}(G)$$

$$\beta \to \gamma\beta^{\sigma}\gamma^{-1}$$

Então $\theta(\alpha) = \gamma\alpha^{\sigma}\gamma^{-1}$ implica que $\sigma^{-1}(\theta(\alpha)) = (\gamma\alpha^{\sigma}\gamma^{-1})^{\sigma^{-1}} = (\alpha^{\sigma})^{\sigma^{-1}} = \alpha$.

Como $\mathbb{Q}$G é semisimples Artiniano, podemos escrever

$$\mathbb{Q}\text{G} = S_1 \oplus S_2 \oplus \ ... \ \oplus S_t,$$

como soma direta de anéis simples S_i. Seja $1 = e_1 + e_2 + ... + e_t$, onde $e_i \in S_i$ são os indempotentes centrais de $\mathbb{Q}G$. Então, como $\sigma^{-1}\theta = id|_{\mathcal{Z}(\mathbb{Q}G)}$ temos

$$S_i = e_i\mathbb{Q}\text{G} \quad \text{e} \quad (\sigma^{-1}\theta) \ (S_i) = S_i, \quad 1 \leq i \leq t.$$

Como $\sigma^{-1}\theta$ mantém o centro de S_i fixo, ele atua em S_i como um automorfismo interno por algum $\alpha_i \in S_i$. Segue que $\sigma^{-1}\theta$ é um automorfismo interno de $\mathbb{Q}$G por $\alpha = \alpha_1 + \alpha_2 + ... + \alpha_t$. Assim, temos que para $g \in G$:

$$\sigma^{-1}\theta(g) = \alpha g \alpha^{-1} \ ; \ \theta(g) = \gamma g^{\sigma}\gamma^{-1} \ ; \text{ onde } \gamma = \sigma(\alpha).$$

□

Lema 2.2. *Seja G um grupo nilpotente de classe dois. Então as somas de classe K_g são da forma $g\hat{H}$, onde H é um subgrupo do grupo derivado G'.*

Demonstração. Como G é um grupo nilpotente de classe dois então temos que

$$\{1\} \lhd G \lhd \mathcal{Z}(G) \lhd G.$$

Seja $H = \{h^{-1}gh \ ; \ h \in G\}$, então $g^{-1}h^{-1}gh = e_h \ \in \mathcal{Z}(G)$, pois $G' \subset \mathcal{Z}(G)$, o que implica $h^{-1}gh = e_h g$ com $e_h \in \mathcal{Z}(G)$. Portanto,

$$K_g = \sum_{h\in G} h^{-1}gh = \sum_{h\in G} e_h g = \sum_{h\in G} g e_h = g\sum_{h\in G} e_h = g\widehat{H},$$

pois o conjunto dos $e_{h's}$ é subgrupo de G. Vamos agora provar esta última afirmação. Seja $e_{h_1} = h_1^{-1}gh_1g^{-1}$ e $e_{h_2} = h_2^{-1}gh_2g^{-1}$, então

$$e_{h_1}e_{h_2} = h_1^{-1}gh_1g^{-1}h_2^{-1}gh_2g^{-1} = h_2^{-1}h_1^{-1}gh_1g^{-1}gh_2g^{-1} =$$

$$= h_2^{-1}h_1^{-1}gh_1h_2g^{-1} = (h_1h_2)^{-1}g(h_1h_2)g^{-1} = e_{h_1h_2}$$

que é um dos $e_{h's}$. Agora seja $e_{h_1} = h_1^{-1}gh_1g^{-1}$ multiplicando por gg^{-1} em ambos os lados dos dois lados da igualdade temos que $eh_1{}^{-1}$ também é um dos $e_{h's}$, o que termina nossa prova. □

Proposição 2.3. *Seja μ um automorfismo de $\mathbb{Z}G$, onde G é um grupo nilpotente de classe dois. Sejam K_i ,$1 \leq i \leq r$, as somas de classe de G. Suponha que $\mu(K_i) = K_{i'}$; $1 \leq i \leq r$. Então existe um automorfismo σ de G o qual, quando extendido para $\mathbb{Z}G$, satisfaz $\sigma(K_i) = K_{i'}$, para todo $1 \leq i \leq r$.*

Demonstração. Pelo lema anterior, temos que as somas de classe de um grupo nilpotente de classe dois são da forma $g\hat{H}$; onde $\hat{H} = \sum_{h\in H} h$ e H é um subgrupo do grupo derivado G'. Seja $\mu(g) = \gamma$. Então

$$\mu(K_g) = \mu(g\widehat{H}) = \gamma\hat{H}_1$$

onde H_1 é um outro subgrupo do grupo derivado G'. Agora

$$\gamma\hat{H}_1 = K_{g_1} = g_1\hat{H}_2.$$

Afirmamos que $H_1 = H_2$. Observe que

$$|H_1|g_1\hat{H}_2 = |H_1|\gamma\hat{H}_1 = \gamma\hat{H}_1\hat{H}_1 = g_1\hat{H}_2\hat{H}_1$$

e então temos $|H_1|\hat{H}_2 = \hat{H}_2\hat{H}_1$. Portanto $H_1 \subset H_2$, pois se $H_1 \not\subset H_2$, isto é, existe um $h \in H_1$ tal que $h \notin H_2$. Como

$$supp\ (\hat{H}_2\hat{H}_1) = \{h_2h_1\ ;\ h_2 \in H_2 \quad e \quad h_1 \in H_1\}$$

temos que $h_2h \in supp(\hat{H}_2\hat{H}_1)$ onde $h \in H_1$ mas $h \notin H_2$ o que implica que $h_2h \notin supp(|H_1|\hat{H}_2)$ e então $supp(\hat{H}_2\hat{H}_1) \not\subset supp(|H_1|\hat{H}_2)$. Analogamente podemos provar que $H_2 \subset H_1$ e concluimos que $H_1 = H_2$. Assim, temos que $\mu(K_g) = \gamma\hat{H}_1 = g_1\hat{H}_1$. Nós afirmamos que existe um $g_2 \in G$ tal que $\gamma \equiv g_2$ mod $\Delta(H_1)\Delta(G)$. Como $\gamma\hat{H}_1 = g_1\hat{H}_1$, temos que

$$\gamma = g_1 + \sum(1-h)t(h) \ .$$

Para simplificar a notação, denotaremos por $\Delta(H_1)$ o ideal $\Delta(G, H_1)$.
Temos então que

$$g_1 + \textstyle\sum_{h\in H_1}(1-h)t(h) \equiv g_1 + \sum_{h\in H_1}(1-h)n_h \text{ mod } \Delta(H_1)\Delta(G),$$

onde $n_h \in \mathbb{Z}$. Basta escolhermos $\varepsilon(t(h)) = n_h$, onde ε é a função de aumento .
Agora vamos mostrar que

$$g_1 + \sum_{h\in H_1}(1-h)n_h \equiv g_1 + 1 - \prod_{h\in H_1} h^{n_h} \text{ mod } \Delta(H_1)\Delta(G).$$

Para isso vamos fazer um construção passo a passo. Primeiro, tomemos $a \in H_1$ e $b \in G$ e primeiro observe que:

$$(1-ab) = -(1-a)(1-b) + (1-a) + (1-b), \text{ se e somente se,}$$
$$(1-ab) - (1-a) - (1-b) \in \Delta(H_1)\Delta(G), \text{ isto é,}$$
$$(1-ab) \equiv (1-a) + (1-B) \ \ mod\Delta(H_1)\Delta(G).$$

Analogamente, temos que

$$(1-a^{n_1}b^{n_2}) = -(1-a^{n_1})(1-b^{n_2}) + (1-a^{n_1}) + (1-b^{n_2}), \text{ se e somente se,}$$
$$(1-a^{n_1}b^{n_2}) - (1-a^{n_1}) - (1-b^{n_2}) \in \Delta(H_1)\Delta(G), \text{ isto é,}$$

$$(1-a^{n_1}b^{n_2}) \equiv (1-a^{n_1}) + (1-b^{n_2}) \ \ mod\Delta(H_1)\Delta(G). \tag{2.1}$$

E também temos

$$(1-a^{n_1}) = -(1-a^{n_1-1})(1-a) + (1-a^{n_1-1}) + (1-a), \text{ se e somente se,}$$
$$(1-a^{n_1}) - (1-a^{n_1-1}) - (1-a) \in \Delta(H_1)\Delta(G), \text{ isto é,}$$

$$(1-a^{n_1}) \equiv (1-a^{n_1-1}) + (1-a) \ \ mod \Delta(H_1)\Delta(G). \tag{2.2}$$

Temos então que

$$(1-a^{n_1}) \equiv (1-a^{n_1-2}) + (1-a)2 \ \ mod \Delta(H_1)\Delta(G), \text{ pois}$$

$$(1-a^{n_1-1}) \equiv (1-a^{n_1-2}) + (1-a) \ \ mod \Delta(H_1)\Delta(G).$$

O que motiva a provar a seguinte afirmação:

$$(1-a^{n_1}) \equiv (1-a^{n_1-i}) + (1-a)i \ \ mod \Delta(H_1)\Delta(G), \ com \ \ i \in \{1, 2..., n_1\}. \tag{2.3}$$

Usaremos indução em i, para provar a afirmação. Para $i = 1$ já provamos anteriormente em 2.2.

Suponha que

$$(1-a^{n_1}) \equiv (1-a^{n_1-(n_1-1)}) + (1-a)(n_1-1) \ \ mod \Delta(H_1)\Delta(G), \text{ isto é,}$$
$$(1-a^{n_1}) - (1-a^{n_1-(n_1-1)}) - (1-a)(n_1-1) \in \Delta(H_1)\Delta(G), \text{ mas}$$

$$(1-a^{n_1}) - (1-a^{n_1-(n_1-1)}) - (1-a)(n_1-1) =$$

$$= (1-a^{n_1}) - (1-a) - (n_1 - 1 - an_1 - a) =$$

$$= (1-a^{n_1}) - (1-a) - n_1 + 1 + an_1 + a =$$

$$= (1-a^{n_1}) - (1-a)n_1.$$

Portanto,

$$(1-a^{n_1}) - (1-a)n_1 \in \Delta(H_1)\Delta(G), \text{ isto é,}$$

$$(1-a^{n_1}) \equiv (1-a)n_1 \ mod \Delta(H_1)\Delta(G). \tag{2.4}$$

O que prova nossa afirmação.

Logo, por 2.1 e 2.4, podemos concluir que

$$(1 - a^{n_1}b^{n_2}) \equiv (1-a)n_1 + (1-b)n_2 \text{ mod } \Delta(H_1)\Delta(G) \ .$$

Agora vamos provar que

$$(1 - \prod_{i=1}^{|H|} a_i^{n_i}) \equiv \sum_{i=1}^{|H|} n_i(1-a_i) \ mod \Delta(H_1)\Delta(G).$$

Por 2.4, temos para $i = 1$ que a equivalência abaixo é verdadeira,

$$(1 - a_1^{n_1}) \equiv n_1(1-a_1) \ mod \Delta(H_1)\Delta(G).$$

Suponha verdadeira a equivalência abaixo,

$$(1 - \prod_{i=1}^{|H|-1} a_i^{n_i}) \equiv \sum_{i=1}^{|H|-1} n_i(1-a_i) \ mod \Delta(H_1)\Delta(G). \tag{2.5}$$

Como

$$(1 - \prod_{i=1}^{|H|} a_i^{n_i}) = -(1 - \prod_{i=1}^{|H|-1} a_i^{n_i})(1 - a_{|H|}^{n_{|H|}}) + (1 - \prod_{i=1}^{|H|-1} a_i^{n_i}) + (1 - a_{|H|}^{n_{|H|}})$$

se e somente se,

$$(1 - \prod_{i=1}^{|H|} a_i^{n_i}) - (1 - \prod_{i=1}^{|H|-1} a_i^{n_i}) - (1 - a_{|H|}^{n_{|H|}}) \in \Delta(H_1)\Delta(G),$$

isto é,

$$(1 - \prod_{i=1}^{|H|} a_i^{n_i}) \equiv (1 - \prod_{i=1}^{|H|-1} a_i^{n_i}) + (1 - a_{|H|}^{n_{|H|}}) \ mod \Delta(H_1)\Delta(G)$$

Então usando a hipótese de indução 2.5, temos que

$$(1 - \prod_{i=1}^{|H|} a_i^{n_i}) \equiv \sum_{i=1}^{|H|-1} n_i(1-a_i) + (1 - a_{|H|}^{n_{|H|}}) \ mod \Delta(H_1)$$

Portanto,

$$(1-\prod_{i=1}^{|H|} a_i^{n_i}) \equiv \sum_{i=1}^{|H|} n_i(1-a_i)\ mod \Delta(H_1)\Delta(G),$$

pois facilmente podemos verificar utilizando o mesmo raciocínio de 2.1, 2.2 e 2.4 que

$$(1-a_{|H|}^{n_{|H|}}) \equiv n_{|H|}(1-a_{|H|}).$$

Concluimos então que

$$g_1 + \sum_{h\in H_1}(1-h)n_h \equiv g_1 + 1 - \prod_{h\in H_1} h^{n_h} \text{ mod } \Delta(H_1)\Delta(G).$$

Vamos mostrar mais um equivalência. Na realidade, queremos mostrar que

$$g_1 + 1 - \textstyle\prod_{h\in H_1} h^{n_h} \equiv g_1 \prod_{h\in H_1} h^{-n_h} \text{ mod } \Delta(H_1)\Delta(G).$$

Observe primeiro que a e $b \in H_1$ e $g_1 \in G$ podemos afirmar que

$$a^{-1}b^{-1}ab = 1.$$

De fato, $a^{-1}b^{-1}ab \in [H,H] \subseteq [G',G'] = G'' = \{1\}$,pois por hipótese G é grupo nilpotente de classe dois. Então podemos fazer o seguinte:

$$g_1(a^{-1}b^{-1}) = -(1-g_1(a^{-1}b^{-1}))(1-ab) + g_1 + (1-ab), \text{ se e somente se,}$$
$$g_1(a^{-1}b^{-1}) - g_1 - (1-ab) \in \Delta(H_1)\Delta(G), \text{ isto é,}$$
$$g_1(a^{-1}b^{-1}) \equiv g_1 + (1-ab)\ mod \Delta(H_1)\Delta(G)$$

Analogamente, temos

$$(a^{n_1}b^{n_2})((a^{n_1})^{-1}(b^{n_2})^{-1}) = 1,$$

pois G é grupo nilpotente de classe dois. Então podemos fazer o seguinte:

$$g_1((a^{n_1})^{-1}(b^{n_2})^{-1}) = -(1-g_1((a^{n_1})^{-1}(b^{n_2})^{-1}))(1-a^{n_1}b^{n_2}) + g_1 + (1-a^{n_1}b^{n_2}),$$

se e somente se,

$$g_1((a^{n_1})^{-1}(b^{n_2})^{-1}) - g_1 - g_1((a^{n_1})^{-1}(b^{n_2})^{-1}) \in \Delta(H_1)\Delta(G), \text{ isto é,}$$
$$g_1((a^{n_1})^{-1}(b^{n_2})^{-1}) \equiv g_1 + g_1(a^{n_1})^{-1}(b^{n_2})^{-1}) \; mod \Delta(H_1)\Delta(G).$$

Como

$$g_1 + 1 - \prod_{i=1}^{|H|} a_i^{-n_i} = -(1 - g_1 \prod_{i=1}^{|H|} a_i^{-n_i})(1 - \prod_{i=1}^{|H|} a_i^{n_i}) - g_1(\prod_{i=1}^{|H|} a_i^{-n_i}),$$

temos que

$$g_1 + 1 - \prod_{i=1}^{|H|} a_i^{-n_i} + g_1(\prod_{i=1}^{|H|} a_i^{-n_i}) \in \Delta(H_1)\Delta(G),$$

isto é,

$$g_1 + 1 - \prod_{i=1}^{|H|} a_i^{-n_i} \equiv g_1(\prod_{i=1}^{|H|} a_i^{-n_i}) \; mod \Delta(H_1)\Delta(G).$$

Finalmente, concluimos que

$$g_1 + 1 - \prod_{h \in H_1} h^{n_h} \equiv g_1 \prod_{h \in H_1} h^{-n_h} \mod \Delta(H_1)\Delta(G).$$

Assim, temos que $\gamma \equiv g_2 \mod \Delta(H_1)\Delta(G)$ e então $\gamma \equiv g_2 \mod \Delta(G')\Delta(G)$, pois $H_1 \subset G'$. Nós afirmamos que dado γ como acima existe um único $g_\gamma \in G$ tal que $\gamma \equiv g_\gamma \mod \Delta(G')\Delta(G)$ e que

$$\lambda \; : \mu(G) \longrightarrow G$$
$$\gamma \longmapsto g_\gamma$$

é um isomorfismo. De fato, suponha que exista um $g_1 \in G$ tal que $\gamma \equiv g_1 \mod \Delta(G')\Delta(G)$. Como $\gamma \equiv g_2 \mod \Delta(G')\Delta(G)$ temos que $g_1 - g_2 \equiv 0 \mod \Delta(G')\Delta(G)$ então $g_1(1-g_1^{-1}g_2) \equiv 0 \mod \Delta(G')\Delta(G)$ o que implica $(1-g_1^{-1}g_2) \equiv 0 \mod \Delta(G')\Delta(G)$ se e só se $g_1^{-1}g_2 - 1 = 0$, pois $(1 - g_1^{-1}g_2)$ é um elemento da base $\Delta(G)$. Portanto $g_1 = g_2$. E λ como acima é um isomorfismo de $\mu(G)$ em G

pois μ é um automorfismo de $\mathbb{Z}(G)$, o que prova nossa afirmação. Pela unicidade, segue que $g_\gamma = g_2$. Como $\gamma \equiv g_\gamma \mod \Delta(H_1)\Delta(G)$, temos que $g_\gamma \hat{H}_1 = \gamma \hat{H}_1$. Seja $\sigma(g) = \lambda(\mu(g))$. Então σ é um automorfismo de G e

$$\sigma(K_g) = \lambda(\mu(K_g)) = \lambda(\gamma \hat{H}_1) = \lambda(\gamma)\hat{H}_1 = g_\lambda \hat{H}_1 = \gamma \hat{H}_1 = \mu(K_g) = K'_g.$$

Isto completa a prova.

□

Agora, vamos provar o resultado principal desse capítulo.

Teorema 2.4. *Seja θ um automorfismo de $\mathbb{Z}G$, onde G é um grupo nilpotente de classe dois. Então existe um automorfismo de σ de G e uma unidade γ de $\mathbb{Q}(G)$ tal que $\theta(g) = \pm\gamma g^\sigma \gamma^{-1}$; para todo $g \in G$.*

Demonstração. Seja

$$\alpha = \textstyle\sum_{g\in G} \alpha_g g \in \mathbb{Z}(G) \text{ e } \varepsilon(\alpha) = \sum_{g\in G} \alpha_g,$$

onde ε é a função de aumento. É claro que $\varepsilon(\theta(g)) = \pm 1$, para qualquer elemento $g \in G$. Normalize θ definindo $\mu(g) = \varepsilon(\theta(g))\theta(g)$. Estenda μ linearmente para $\mathbb{Z}G$ e dete modo μ torna-se um automorfismo de $\mathbb{Z}G$ o qual aplica somas de classe em somas de classe, este fato segue do teorema de Glauberman. Como, por hipótese, G é um grupo nilpotente de classe dois, temos pela proposição anterior existe um automorfismo de σ de G, o qual estendido para $\mathbb{Z}(G)$ satisfaz $\sigma(K_i) = \pm K_{i'}$ e que pela proposição 2.1 segue que podemos acha uma unidade de $\mathbb{Q}(G)$ tal que $\theta(g) = \pm\gamma g^\sigma \gamma^{-1}$; para todo $g \in G$. □

Capítulo 3

Isomorfismos dos anéis de grupos inteiro de grupos abelianos finitamente gerados

Em 1940, **G.Higman** provou que toda unidade de ordem finita do anel de grupo $\mathbb{Z}G$ de um grupo abeliano finito é da forma $\pm g$, $g \in G$. E este resultado usou para provar que :

Sejam G e H grupos abelianos finitos então $\mathbb{Z}G \simeq \mathbb{Z}H$ implica $G \simeq H$.

Neste capítulo, vamos extender este resultado para grupos abelianos finitamente gerados. Para isso, assim como **G.Higman**, primeiro caracterizaremos as unidades de ordem finita do anel de grupo $\mathbb{Z}G$ de um grupo abeliano finitamente gerado.

Lema 3.1. *Toda unidade de ordem finita no anel de grupo $\mathbb{Z}G$ de um grupo abeliano arbitrário G é da forma $\pm t$, onde t é um elemento de torção de G.*

Demonstração. Substituindo G pelo subgrupo gerado pelo $supp(\gamma)$, onde γ é uma unidade de ordem finita de $\mathbb{Z}G$, podemos supor sem perda de generalidade que G é finitamente gerado. Escreva $G = T \times F$, onde T é o subgrupo torção de G e F é livre. Além disso, $F = \langle x_1 \rangle \times \langle x_2 \rangle \times ... \langle x_l \rangle$.Um elemento de G pode ser escrito de forma única como $g = t.x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} ... x_l^{\alpha_l}$, onde $\alpha_i \in \mathbb{Z}$ e $t \in T$. Defina $d_i(g) = |\alpha_i|$. Suponha que

$$\gamma = m_1 g_1 + m_2 g_2 + ... + m_s g_s$$

é tal que $\gamma^n = 1$. Então temos que provar que $\gamma = \pm t \in G$. Seja

$$n_i = \max_{1 \leqq j \leqq s} d_i(g_j)$$

Assim, devemos usar o grupo

$$H = \langle x_1^{2n_1+1} \rangle \times \langle x_2^{2n_2+1} \rangle ... \times \langle x_l^{2n_l+1} \rangle$$

o qual tem índice finito em G. Claramente, $(\overline{\gamma})^n = 1$, onde $\overline{\gamma}$ é a imagem de γ na projeção $\mathbb{Z}G \to \mathbb{Z}(G/H)$, e pelo resultado de Higman temos que $\overline{\gamma} = \pm xH$, $x \in G$. Como $g_1, g_2, ..., g_s$ pertencem a diferentes classes de H, temos que $\gamma = \pm g_i$, onde $g \in T$. □

Precisaremos de mais um lema para provar o teorema.

Lema 3.2. *Se A é um grupo abeliano livre de torção e K é um corpo, então KA não contém divisores de zero.*

Demonstração. Sejam μ,$\gamma \in KA - \{0\}$ tal que $\mu\gamma = 0$. Então, substituindo A pelo grupo gerado por $supp(\mu) \cup supp(\gamma)$, podemos supor que A é finitamente gerado. Como A é livre de torção, temos um decomposição

$$A = \langle x_1 \rangle \times \langle x_2 \rangle \times ... \langle x_n \rangle$$

para alguns elementos $x_i \in A$, $1 \leqq i \leqq n$. Então, KA pode ser mergulhado no corpo $K(X_1, ..., X_n)$ das funções racionais nas variáveis $X_1, ..., X_n$ sobre K, que é um domínio de integridade. □

Agora vamos provar o resultado o qual nos referimos no início deste capítulo.

Teorema 3.3. *Suponha que G e H são grupos abelianos finitamente gerados. Então $\mathbb{Z}G \simeq \mathbb{Z}H$ implica $G \simeq H$.*

Demonstração. Escreva $G = T \times \langle x_1 \rangle \times ... \times \langle x_l \rangle$ e $H = T_1 \times \langle y_1 \rangle \times ... \times \langle y_m \rangle$ como no lema 3.1. Seja $\theta : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo. Para $t \in T$, seja $\mu(t) = t_1 \in T_1$ se $\theta(t) = \pm t_1$ e seja $\mu(x_i) = \theta(x_i)$. Estendendo linearmente, obtemos um isomorfismo $\mu : \mathbb{Z}G \to \mathbb{Z}H$ tal que $\mu(T) = T_1$. Logo,

$$\mathbb{Z}(G/T) \simeq \mathbb{Z}(H/T_1).$$

Pelo lema 3.2 $\mathbb{Q}(G/T)$ não tem divisores de zero. Como $\mathbb{Z}(G/T) \subset \mathbb{Q}(G/T)$ temos que $\mathbb{Z}(G/T)$ é livre de divisores de zero, logo $\mathbb{Z}(G/T)$ é um Domínio de Integridade. Assim podemos contruir seu corpo quociente. E temos que o corpo quociente de $\mathbb{Z}(G/T)$ é $\mathbb{Q}(G/T)$.

Observe que $G/T = \langle x_1 \rangle \times ... \times \langle x_l \rangle$ é livre de torção, então $\mathbb{Q}(G/T)$ pode ser mergulhado no corpo $\mathbb{Q}(x_1, ..., x_l)$ das funções racionais nas variaveis $x_1, ..., x_l$ sobre $\mathbb{Q}$. O grau de transcendência de $\mathbb{Q}(x_1, ..., x_l)$ sobre $\mathbb{Q}$ é l, então o grau de transcendência de $\mathbb{Q}(G/T)$ sobre $\mathbb{Q}$ é l, isto é, $x_1, ..., x_l$ é uma base de $\mathbb{Q}(G/T)$ sobre $\mathbb{Q}$. Como $\mathbb{Z}(G/T) \subset \mathbb{Q}(G/T)$, temos que $x_1, ..., x_l$ é uma base de $\mathbb{Z}(G/T)$. Analogamente, podemos provar que $y_1, ..., y_m$ é uma base de $\mathbb{Z}(H/T_1)$. Portanto, $l = m$. Lembrando que anteriormente concluimos que $\mathbb{Z}(G/T) \simeq \mathbb{Z}(H/T_1)$ temos que $G/T \simeq G/T_1$, segue que $G \simeq H$, pois $T \simeq T_1$. □

Capítulo 4

Idempotentes centrais e subgrupos normais

Seja N um subgrupo normal de G; então $\widehat{N} = \sum_{n \in \mathbb{N}} n$ é um elemento central com a propriedade que $\hat{N}^2 = |N|\widehat{N}$. Neste capítulo, caracterizaremos todos $\widehat{N}$ onde N é normal em G com certos elementos de $\mathbb{Z}G$ o qual tem essa propriedade. Além disso, neste capítulo apresentando uma outra demonstração para um fato já demonstrado em [1] e [3], a saber:

> *Se existe um aplicação θ entre o anel de grupo inteiro de um grupo G e o anel de grupo inteiro de um grupo H que é um isomorfismo normalizado, isto é, $\varepsilon(\theta(g)) = 1$ para todo $g \in G$, então existe um correspondência injetiva entre os subgrupos normais de G e H o qual preserva a ordem, a união e a interseção.*

Assumimos que todos os grupos considerados neste capítulo são finitos.

4.1 Fatos Importantes

Lema 4.1. *Dado Y um subconjunto de um grupo G então $\widehat{Y}^2 = m\widehat{Y}$ e $m \in \mathbb{N}$ se e somente se Y é subgrupo de G.*

Demonstração. Suponha que Y não é subgrupo de G, então existem y_1 e $y_2 \in Y$ tais que $y_1y_2 \notin Y$. Por definição temos que

$$supp\ (\widehat{Y}^2) = \{y'y''\ ;\ y'\ e\ y'' \in Y\}$$

então temos que y_1 e $y_2 \in supp\ (\widehat{Y}^2)$. Como $y_1y_2 \notin Y$ temos que $y_1y_2 \notin supp\widehat{Y}$ e assim $supp\ (\widehat{Y}^2) \nsubseteq supp\ (m\widehat{Y})$, o que é uma contradição.

Reciprocamente, assuma que Y é subgrupo de G então

$$\widehat{Y}^2 = \widehat{Y}\widehat{Y} = \left(\sum_{y\in Y} y\right)\widehat{Y} = \sum_{y\in Y}\left(y\widehat{Y}\right) = \sum_{y\in Y}\widehat{Y} = |Y|\widehat{Y}.$$

□

Lema 4.2. *Seja G um grupo então H é um subgrupo normal de G se e somente se $\widehat{H}$ é um elemento central de G.*

Demonstração. Se $H \lhd G$ para qualquer $g \in G$ temos que $g^{-1}Hg = H$; portanto

$$g^{-1}\widehat{H}g = \sum_{h\in H} g^{-1}hg = \sum_{h\in H} h = \widehat{H}.$$

Assim, $\widehat{H}g = g\widehat{H}$, para todo $g \in G$, o que mostra que $\widehat{H}$ é central em G. Reciprocamente, se $\widehat{H}$ é central então $g\widehat{H} = \widehat{H}g$, e assim $g\ supp(\widehat{H}) = supp(\widehat{H})\ g$. Como $supp(\widehat{H}) = H$ temos que $gH = Hg$ e portanto $H \lhd G$. □

Proposição 4.3. *Seja $\gamma = \sum_{g\in G}\gamma_g g$ um elemento central de ZG tal que $\gamma_1 = 1$, $\sum \gamma_g \neq 0$ e $\gamma^2 = m\gamma$, onde m é um número natural. Então*

$$\gamma = \sum_{h\in H} h = \hat{H},$$

onde H é um subgrupo normal de G.

Demonstração. Para um elemento $\alpha = \sum_{g\in G}\alpha_g g$ de $\mathbb{Z}G$, defina

$$\alpha^* = \sum_{g\in G}\alpha_g g^{-1}.$$

Pela proposição 1.11 temos que $(\alpha+\beta)^* = \alpha^* + \beta^*$ e $(\alpha\beta)^* = \beta^*\alpha^*$, e assim, temos que $(\gamma^*)^2 = m\gamma^*$ e que $(\gamma\gamma^*)^2 = m^2\gamma\gamma^*$.

Afirmação 1. $\varepsilon(\gamma) = m$. *De fato, sabemos que*

$$\varepsilon(\gamma) = \varepsilon(\sum_{g\in G}\gamma_g g) = \sum_{g\in G}\gamma_g.$$

Como $\gamma^2 = m\gamma$ *temos que* $\varepsilon(\gamma^2) = \varepsilon(m\gamma)$, *então* $\varepsilon(\gamma)^2 = m\varepsilon(\gamma)$ *e portanto* $\varepsilon(\gamma)(\varepsilon(\gamma) - m) = 0$. *Logo temos somente duas possibilidades: ou* $\varepsilon(\gamma) = 0$ *ou* $\varepsilon(\gamma) = m$, *mas por hipótese* $\varepsilon(\gamma) = \sum_{g\in G}\gamma_g \neq 0$ *concluimos que* $\varepsilon(\gamma) = \sum_{g\in G}\gamma_g = m$ *o que prova nossa afirmação.*

Pelos autovalores (traço) de um elemento α de $\mathbb{Z}G$ entendemos os autovalores (traço) de $[\alpha]$, onde $\alpha \longrightarrow [\alpha]$ é a representação regular de $\mathbb{Z}G$. Claramente γ é diagonalizavel, pois $[\gamma]$ é raiz de $x^2 - mx = 0$ e sabemos que o polinômio minimal divide $x^2 - mx = 0$ e este não tem raizes múltiplas. Como as raizes de $x^2 - mx = 0$ são 0 e m temos que os únicos autovalores possíveis de γ são 0 e m. Dado um elemento α de $\mathbb{Z}G$ vamos denotar o traço desse elemento por $Tr(\alpha)$. Observe que o traço de $g \in G$ se $g \neq 1$ é zero. Como temos $\gamma_1 = 1$ segue que $Tr(\gamma) =$

$$Tr([\gamma]) = Tr\left(\sum_{g\in G}\gamma_g[g]\right) = Tr\left(\gamma_1\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1\end{bmatrix} + \sum_{\substack{g\in G\\ g\neq 1}}\gamma_g[g]\right) =$$

$$= Tr\left(\gamma_1\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1\end{bmatrix}\right) + Tr\left(\sum_{\substack{g\in G\\ g\neq 1}}\gamma_g[g]\right) = |G|$$

Como foi provado anteriormente γ é uma matriz diagonal composta somente de 0's e m's, então o traço de de γ é igual $x.m$, onde m é a quantidade de m's existente na diagonalização de γ. Portanto,

$$Tr[\gamma] = xm = |G|.$$

Por esta razão exatamente $|G| - |G|/m$ autovalores de γ que são zero. Assim, no mínimo, $|G| - |G|/m$ autovalores de $\gamma\gamma^*$ são zero.

$$Tr(\gamma\gamma^*) = Tr([\gamma\gamma^*]) = Tr\left(\sum_{\substack{g,h\in G \\ gh^{-1}=1}} \gamma_g^2[1] + \sum_{\substack{g,h\in G \\ gh^{-1}\neq 1}} \gamma_g\gamma_h[gh^{-1}] \right) =$$

$$= Tr\left(\sum_{\substack{g,h\in G \\ gh^{-1}=1}} \gamma_g^2[1] \right) + Tr\left(\sum_{\substack{g,h\in G \\ gh^{-1}\neq 1}} \gamma_g\gamma_h[gh^{-1}] \right) =$$

$$= Tr\left(\gamma_1^2 \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} + \gamma_{g_1}^2 \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} + ... + \gamma_{g_t}^2 \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \right) =$$

$$= Tr\left(\gamma_1^2 \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}] \right) + Tr\left(\gamma_{g_1}^2 \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \right) + ... +$$

$$+ Tr\left(\gamma_{g_t}^2 \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \right) =$$

$$= \gamma_1^2\ |G|\ +\ \gamma_{g_1}^2\ |G|\ +\ ...\ +\ \gamma_{g_t}^2\ |G|\ =\ |G|\ \sum_{g\in G} \gamma_g^2.$$

Portanto,

$$|G|\ \sum_{g\in G} \gamma_g^2\ =\ Tr(\gamma\gamma^*)\ \leqq m^2\ \frac{|G|}{m}.$$

Concluímos que $\sum_{g \in G} \gamma_g^2 \leqq m = \sum_{g \in G} \gamma_g$ e portanto $\gamma_g = 0$ ou $\gamma_g = 1$. Temos então que $\gamma = \sum_{g \in Y} g$, onde Y é o suporte de γ ,isto é,

$$Y = supp\ (\gamma) = \{g \in G : \gamma_g \neq 0\}.$$

Então, para provarmos que $\gamma = \sum_{h \in H} h$ onde H é subgrupo normal de G, basta provar que Y é um subgrupo normal de G. Observe que $\gamma = \sum_{g \in Y} g = \widehat{Y}$ e como por hipótese temos $\gamma^2 = m\gamma$, então $\widehat{Y}^2 = m\widehat{Y}$. Pelo lema anterior temos que $\widehat{Y}^2 = m\widehat{Y}$ se e somente se Y é subgrupo de G. Segue que Y é subgrupo de G. Como $\gamma = \widehat{Y}$ é central temos que H é normal. □

O teorema que vamos demonstrar agora desempenha um papel fundamental na prova do teorema 4.5.

Teorema 4.4. *Se $u = \sum_{g \in G} u_g g$ é um unidade de ordem finita em RG, e se $u_y \neq 0$ para y no centro de G, então $u = u_y y$ e u_y é uma raiz da unidade.*

Demonstração. Seja u um elemento de RG, isto é,

$$u = \sum_{g \in G} u_g g \in RG$$

e $u \longrightarrow [u]$ a representação regular dos elementos de RG. Pelos autovalores (traço) de um elemento u de RG entendemos os autovalores(traço) de $[u]$. Vamos denotar o traço de um elemento $u \in RG$ por $Tr(u)$. Se u é uma unidade de ordem finita, isto é, $u^n = 1$ temos que $[u^n] = [u]^n = I_d$, onde I_d é a representação regular de 1. Então $[u]$ é diagonalizavel pois o polinômio minimal de $[u]$ divide $x^n - 1$. Portanto,

$$Tr(u) = Tr([u]) = Tr\left(\begin{bmatrix} w_1 & 0 & \cdots & 0 \\ 0 & w_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & w_{|G|} \end{bmatrix}\right) = w_1 + w_2 + ... + w_{|G|}\ ,$$

onde w_i, com $1 \leq i \leq |G|$, são raizes n-ésimas da unidade não necessáriamente distintas. Por outro lado, sabemos que $Tr(u) = u_1|G|$ para qualquer $u \in RG$. Então

$$w_1 + w_2 + ... + w_{|G|} = u_1 \ |G| \ ,$$

o que implica

$$|w_1 + w_2 + ... + w_{|G|}| = | \ u_1 \ |G| \ | = |u_1| \ |G| \ .$$

Como temos $|w_1 + w_2 + ... + w_{|G|}| \leqq |w_1| + |w_2| + ... + |w_{|G|}| = |G|$, pois w_i para cada $i = 1, 2, ..., |G|$ é raiz da unidade e então $|w_i| = 1$. Concluimos que $|u_1| \ |G| \leqq |G|$ e portanto $|u_1| = 0$ ou $|u_1| = 1$. Se $u_1 \neq 0$ então $|u_1| = 1$ e temos que $|w_1 + w_2 + ... + w_{|G|}| = |w_1| + |w_2| + ... + |w_{|G|}|$ se e somente se $w_1 = w_2 = ... = w_{|G|}$. Segue então que

$$[u] = \begin{bmatrix} w_1 & 0 & \cdots & 0 \\ 0 & w_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & w_1 \end{bmatrix}$$

isto é, $[u] = w_1 I_d$; logo $u = w_1 1$. Tome $\bar{u} = uy^{-1}$, onde y está no centro de G e $u_y \neq 0$. Então $\bar{u}$ é uma unidade de ordem finita e pelo que acabamos de demonstrar anteriormente, temos que $\bar{u} = uy^{-1} = w_1 1$ e portanto $u = w_1 y$. □

4.2 Teorema de Preservação e Existência

O teorema a seguir garante que dado um determinado isomorfismo em anéis de grupo inteiros, conseguimos garantir a existência de uma imersão que preserva algumas relações de ordem.

Teorema 4.5. *Seja $\theta : \mathbb{Z}G \to \mathbb{Z}G$ um isomorfismo normalizado, isto é, $\varepsilon(\theta(g)) = 1$ para todo $g \in G$. Então existe uma correspondência injetiva entre os subgrupos normais de G e H que preserva a ordem, a união e a interseção.*

Demonstração. Seja N um subgrupo normal de G. Então $\widehat{N} = \sum_{n \in N} n$ satisfaz $\widehat{N}^2 = |N|\widehat{N}$. Seja $\theta(\widehat{N}) = \gamma = \sum_{g \in G} \gamma_g g$; então $\gamma^2 = |N|\gamma$ e ainda $\varepsilon(\gamma) \neq 0$, pois

$$\varepsilon(\gamma) = \varepsilon(\theta(\widehat{N})) = \varepsilon(\theta(\sum_{n \in N} n)) = \varepsilon(\sum_{n \in N} \theta(n)) = \sum_{n \in N} \varepsilon(\theta(n)) = \underbrace{1 + 1 + ...1}_{n \text{ vezes}} = |N|.$$

Pelo teorema anterior temos que se β é um unidade de ordem finita em $\mathbb{Z}G$ com $\beta_1 \neq 0$ então $\beta = \pm 1$. Portanto, se $\beta = \theta(x)$ com $x \neq e$ temos que $\beta_1 = 0$. Então,

$$\gamma_1 = \theta(\widehat{N})_1 = \theta(\sum_{n \in N} n)_1 = \theta(1)_1 + \theta(n_1)_1 + ... + \theta(n_k)_1 = 1 + 0 + 0 + ... + 0 = 1.$$

Assim, pela proposição 4.3, $\gamma = \theta(\widehat{N}) = \widehat{M}$, onde M é subgrupo normal de H e então, $\widehat{M}^2 = |M| \ \widehat{M}$. Mas $\theta(\widehat{N})^2 = |N| \ \theta(\widehat{N})$ e portanto $|M| = |N|$. Agora, vamos provar que esta correspondência preserva a interseção. Sejam N_1 e N_2 subgrupos normais de G, então $N_1 \cap N_2$ é um subgrupo normal de G e temos que $\theta(\widehat{N_1 \cap N_2}) = \widehat{M_3}$ onde M_3 é subgrupo normal de H. Portanto $N_1 \cap N_2$ tem um correspondente M_3. Agora, falta mostrar que $M_3 = M_1 \cap M_2$, onde M_1 é o correspondente de N_1 e M_2 é o correspondente de N_2, isto é, $\theta(\widehat{N_1}) = \widehat{M_1}$ e $\theta(\widehat{N_2}) = \widehat{M_2}$. Antes de continuarmos observe que;

$$\widehat{N_1}\widehat{N_2} = m\widehat{N_2} \text{ se e somente se } N_1 \text{ é subgrupo de } N_2.$$

Temos então que

$$\widehat{M_3}\widehat{M_1} = \theta(\widehat{N_1 \cap N_2})\theta(\widehat{N_1}) = \theta(\widehat{N_1 \cap N_2}\widehat{N_1}) = \theta(m\widehat{N_1}) = m\theta(\widehat{N_1}) = m\widehat{M_1}.$$

Então M_3 é subgrupo de M_1. Procedendo da mesma maneira podemos provar que $\widehat{M_3}\widehat{M_1} = m'\widehat{M_2}$, e então concluir que M_3 é subgrupo de M_2. Portanto M_3 é subgrupo de $M_1 \cap M_2$. Agora, observemos os seguintes fatos:

fato 1: $supp(\widehat{M_1 \cap M_2}) \subset supp(\widehat{M_1}) = supp(\theta(\widehat{N_1}))$.

fato 2: $supp(\widehat{M_1 \cap M_2}) \subset supp(\widehat{M_2}) = supp(\theta(\widehat{N_2}))$.

Logo, pelos *fato 1* e *fato 2*, temos que

$$supp(\widehat{M_1 \cap M_2}) \subset supp(\theta(\widehat{N_1})) \cap supp(\theta(\widehat{N_2})) = supp(\theta(\widehat{N_1 \cap N_2})) = supp(\widehat{M_3}).$$

Então, $M_1 \cap M_2 \subset M_3$, de onde segue $M_3 = M_1 \cap M_2$. Finalmente vamos provar que esta correspondência preserva a união. Sejam N_1 e N_2 subgrupos normais de G e sejam M_1 o correspendente de N_1 e M_2 o correspendente de N_2, isto é, $\theta(\widehat{N_1}) = \widehat{M_1}$ e $\theta(\widehat{N_2}) = \widehat{M_2}$. Observe os seguintes fatos:

fato 1: $supp(\widehat{M_1}) \subset supp(\theta(\widehat{N_1})) \subset supp(\widehat{M_1 \cup M_2})$.
fato 2: $supp(\widehat{M_2}) \subset supp(\theta(\widehat{N_2})) \subset supp(\widehat{M_1 \cup M_2})$.
fato 3: $supp(\theta(\widehat{N_1 \cup N_2})) \subset supp(\theta(\widehat{N_1})) \cup supp(\theta(\widehat{N_2}))$.

Pelos *fato 1*, *fato 2* e *fato 3*, temos que

$$supp(\theta(\widehat{N_1 \cup N_2})) \subset supp(\theta(\widehat{N_1})) \cup supp(\theta(\widehat{N_2})) \subset supp(\widehat{M_1 \cup M_2}).$$

Por outro lado, temos

$$supp(\theta(\widehat{N_1})) \subset supp(\theta(\widehat{N_1 \cup N_2}) \; e$$

$$supp(\theta(\widehat{N_2})) \subset supp(\theta(\widehat{N_1 \cup N_2}).$$

Então,

$$supp(\widehat{M_1 \cup M_2}) \subset supp(\widehat{M_1}) \; \cup \; supp(\widehat{M_2}) =$$

$$supp(\theta(\widehat{N_1})) \; \cup \; supp(\theta(\widehat{N_2})) \subset supp(\theta(\widehat{N_1 \cup N_2})).$$

Logo, $supp(\theta(\widehat{N_1 \cup N_2})) = supp(\widehat{M_1 \cup M_2})$ e portanto $\theta(\widehat{N_1 \cup N_2}) = \widehat{M_1 \cup M_2}$.

□

Referências Bibliográficas

[1] Conh, J.A. e Livingstone, D., *On the structure of group algebra.* I, can J. Math. *17* (1965), 583 - 593.

[2] Higman, Graham., *The units of group rings,* Proc. London Math. Soc. *46* (1940), 231 - 248.

[3] Passman, D. S., *Isomorphic groups and group rings,* Pacific J. Math. *15* (1965), 561 - 583.

[4] Jackson,D. A., Ph. D. Thesis, Oxford University, Oxford, 1967.

[5] Waerden, B. L. van der, *Modern algebra,* (Ungar, *New York*, 1950).

[6] Whitcomb,A., Ph. D. Thesis, University of Chicago, Illinois, 1967.

[7] Cayley, A.,*On the Theory of Groups as Depending on the Symbolic Equation* $\theta^n = 1$, Phil. Mag., 7(1854), 40 - 47.

[8] Polcino Miles, César and Sehgal, Sudarshan K., *An Introdution to Group Rings. Kluwer Academic Publishers, 2002.*

[9] Sehgal, Sudarshan K., *On the isomorphism of integral group rings. I* Can. J. Math, 21 (1969),410-413.